CDPH INFORMATION SECURITY OFFICE (ISO)
INFORMATION SECURITY INCIDENT
DETERMINATION CHECKLIST

Public Health Administrative Manual (PHAM)
CDPH Information Security Policies
State Administrative Manual (SAM) Section 5300
Penal Code section 502(c)

Date Reported:
Reported By:

#	YES	NO	TYPE OF MEDIUM
1.	☐	☐	Electronic data (includes e-mails, faxes)
2.	☐	☐	Encrypted
3.	☐	☐	Paper
4.	☐	☐	Oral

#	YES	NO	INFORMATION SECURITY VIOLATIONS – STATE DATA
1.	☐	☐	Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive, or personal. (State Administrative Manual (SAM) Section 5320.5)
2.	☐	☐	Deliberate or accidental distribution or release of personal information by a Department, its employee(s), or its contractor(s) in a manner not in accordance with law or policy.
3.	☐	☐	Intentional non-compliance by the Information Custodian of information within his/her responsibilities. (SAM Section 5320.3)

#	YES	NO	INFORMATION SECURITY VIOLATIONS – INAPPROPRIATE USE & UNAUTHORIZED ACCESS
1.	☐	☐	State Employee
2.	☐	☐	Non-State Employee
3.	☐	☐	**Tampering** with State computer data and computer systems.
4.	☐	☐	**Interference** with State computer data and computer systems.
5.	☐	☐	**Damage** to State computer data and computer systems.
6.	☐	☐	**Unauthorized access** to State computer data and computer systems.

#	YES	NO	INFORMATION SECURITY VIOLATIONS – EQUIPMENT
1.	☐	☐	**Theft** of State-owned IT equipment or any electronic devices containing or storing

			confidential, sensitive, or personal data.
2.	☐	☐	**Damage or destruction** of State-owned IT equipment or any electronic devices containing or storing confidential, sensitive, or personal data.
3.	☐	☐	**Loss** of State-owned IT equipment or any electronic devices containing or storing confidential, sensitive, or personal data.

#	YES	NO	INFORMATION SECURITY VIOLATIONS – COMPUTER CRIME
1.	☐	☐	Any individual knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
2.	☐	☐	Any individual knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
3.	☐	☐	Any individual knowingly and without permission uses or causes to be used computer services.
4.	☐	☐	Any individual knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
5.	☐	☐	Any individual knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
6.	☐	☐	Any individual knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
7.	☐	☐	Any individual knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
8.	☐	☐	Any individual knowingly introduces any computer contaminant into any computer, computer system, or computer network.
9.	☐	☐	Any individual knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a

CDPH INFORMATION SECURITY OFFICE (ISO)
INFORMATION SECURITY INCIDENT
DETERMINATION CHECKLIST

Public Health Administrative Manual (PHAM)
CDPH Information Security Policies
State Administrative Manual (SAM) Section 5300
Penal Code section 502(c)

#	YES	NO	INFORMATION SECURITY VIOLATIONS – COMPUTER CRIME
			computer, computer system, or computer network.

#	YES	NO	INFORMATION SECURITY VIOLATIONS – DEPARTMENT POLICY
1.	☐	☐	Access was not terminated immediately for exiting staff. (InfoSec Policy - Section 140)
2.	☐	☐	Content placed on the Internet was not approved in accordance with existing information release policies and procedures prior to placement on the Internet and/or E-mail. (InfoSec Policy - Section 140)
3.	☐	☐	Classified data was released by the Department to external entities in violation of Federal or State laws or regulations, or Department policies, and without approval by the CISO and the Privacy Officer. (InfoSec Policy - Section 140)
4.	☐	☐	Individuals other than Department employees were granted access to the Department network or any State computer systems without obtaining prior approval from both the Division Chief overseeing those individuals and the ISO. (InfoSec Policy - Section 140)
5.	☐	☐	Remote control software was installed and/or used without completion of a formal risk analysis and written approval by the ISO. (InfoSec Policy - Section 240)
6.	☐	☐	Unauthorized use of a user ID or password. (InfoSec Policy - Section 820)
7.	☐	☐	Any violation of the Acceptable Use of Information Technology Resources section. (InfoSec Policy - Section 1900)
8.	☐	☐	Other –Any other violation of Department policy, including Public Health Administrative Manual (PHAM), or CDPH ISO Information Security Policies.
If #8, Policy and Section violated:			